The Report committee for Janel Eden Yost

Certifies that this is the approved version of the following report:

Physical crimes informed by publicly available identity information: Underreported risk or overhyped myth?

APPROVED BY

SUPERVISING COMMITTEE:

_____

Paul Adams, Supervisor

_____

Craig Blaha

Physical crimes informed by publicly available identity information: Underreported risk or overhyped myth?

by

Janel Eden Yost

Report

Presented to the Faculty of the Graduate School

of the University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

Master of Science in Identity Management and Security

The University of Texas at Austin

December 2017

Physical crimes informed by publicly available identity information: Underreported risk or overhyped myth?

by

Janel Eden Yost, MSIMS

The University of Texas at Austin, 2017

SUPERVISOR: Paul Adams

Vulnerabilities associated with the wide dissemination of personally identifiable information (PII) are well documented from an identity theft perspective, but reporting of identity-related crimes that result in assaults, robberies, and other physical losses has been inconsistent. This paper aims to identify gaps in existing research regarding physical crimes informed by the public availability of PII, with an emphasis on vulnerabilities created by victim self-publication of identity information through social media. A survey of media reporting regarding 111 recent incidents, or strings of connected incidents, has facilitated the establishment of rudimentary patterns in these crimes, as well as trends in reporting, both within the US and abroad. A review of pop culture commentary on the current risk environment offers insights into public perceptions of risk, and how these perceptions may be impacted by the media and entertainment industries.

Contents

Introduction

Personally identifiable information (PII) is a high-value asset that is difficult to protect, relatively easy to acquire, and exploitable for a variety of purposes. The identity theft related vulnerabilities associated with PII are well documented. Numerous organizations are currently engaged in identity theft and fraud research. The *2017 Identity Fraud Study* published by Javelin Strategy & Research indicates that the incidence of identity fraud events in the U.S. rose 16 percent from 2015 to 2016, reporting a record high of 15.4 million victims in 2016 (Identity Fraud, 2017). The University of Texas at Austin's Center for Identity has built an Identity Threat Assessment and Prediction model which utilizes data gathered from over 5,000 identity theft incidents to provide "unique, research-based insights into the habits and methods of identity threats, and… uncovers the identity attributes most vulnerable to theft, assesses their importance, and determines the personally identifiable information (PII) most frequently targeted by thieves and fraudsters" (Identity Theft, 2017, p. 3).

While the aforementioned efforts are extremely important in the current environment of ever-increasing threats to identity, this research focuses exclusively on the financial, and to a lesser degree emotional, impacts of identity theft. Far less research has been conducted to date regarding the physical risks associated with the public disclosure of identity information, and how individuals' perceptions of risk may impact their actual risk. The intent of this report is not so much to draw specific conclusions regarding physical crimes informed by publicly available identity information, as it is to (1) identify whether or not these types of crimes are actually

occurring, and (2) survey the current climate and identify areas where further research may be warranted.

This report addresses four specific areas:

1. Current challenges concerning public access to critical identity-related information of two types; personal information, the availability of which creates vulnerabilities, and crime reporting information, the lack of which may be a disservice to the public. Despite distinct differences in circumstances and outcomes, the crimes surveyed for this report have two things in common; they were all informed by publicly available identity information, and many media reports regarding these crimes are vague. These two commonalities identify gaps in existing research. First, why is the information reported about these incidents so vague? Is it an intentional effort on the part of law enforcement to try and limit copycat crimes, is it due to a general disinterest on the part of media, or is there some other reason? Also unaddressed by existing research is what impact, if any, does this lack of reporting have on the general public's ability to protect themselves from future similar incidents?
2. The identification of patterns regarding crimes associated with social media and other publicly available identity information, such as types of crimes committed, frequency, and specific sources of information criminals used to target their victims. While this report touches upon patterns with regards to victim gender, other patterns which could be

investigated by researchers in the future include examining the geographic location of crimes, analyzing social media use patterns among victims to determine if there are any correlations between an individual's level of social media activity and the likelihood that they will become a victim, as well as patterns in socioeconomic factors related to both victims and perpetrators, including age, education, income, and employment status.

3. How these crimes are reported by the media, including which outlets are regularly reporting such crimes; the local, regional, national, or international dissemination of crime reports; differences in reporting between the US and elsewhere in the world; and the manner in which news of specific incidents is conveyed, i.e. are risks under reported, or overhyped to the point of causing people to become desensitized?
4. The general public's perception of risk associated with publicly available identity information and the over-sharing of such information on social media, the degree to which public opinion is polarized regarding these issues, and what role the media and entertainment industries play in framing these perceptions.

Current Challenges Contributing to the Threat Environment

Numerous challenges currently exist in the realm of PII, including the availability and ease of access to information, the 21st century information sharing culture, the increased use of mobile applications, and a general lack of awareness regarding the relatively new risks brought about in the digital environment. A survey of specific criminal incidents demonstrates that these challenges are repeatedly seen as contributing factors in crimes that began with a criminal utilizing readily available PII to target an individual, and ended with assault, rape, murder, or some other physical loss.

Information Ease of Access

Even in the absence of hacking, phishing, and other cyber-related attempts to access restricted PII, the amount of identity information that is freely and openly available to the public regarding the average American is astonishing. Address histories, telephone numbers, email addresses, dates of birth, close relatives and associates, voter registration records, political campaign contributions, motor vehicle purchase information, real property records, business filings, professional licenses, court and criminal records, and marriage and divorce records are but a few examples of the types of information that can be easily accessed by anyone, and often obtained for free. Alternately, would-be criminals who are not motivated enough to track down information from original sources have the option of paying a small fee for aggregated "comprehensive reports" of a variety of records such as employment, education, social networking, criminal, lien, and marriage records from data resellers such as Spokeo and BeenVerified. Whereas major data aggregators such as LexisNexis and Thomson

Reuters limit direct access to their databases, there is no client vetting involved with the lower-level resellers; these companies will sell PII to anyone with an Internet connection and a credit card.

Ironically, the websites of some of these data resellers, such as Intelius, offer unlimited access to "the most accurate and updated information from billions of records" for sale, right next to offers of identity protection services (Want, n.d.). In "Without Permission: Privacy on the Line," Pratt and Conger detail the lack of regulation and the legal grey areas in the dissemination of information by third and fourth parties, asserting that "legal compliance is via self-regulation" and that many third and fourth party vendors apply very broad interpretations of what are legitimate business purposes and permissible uses, or they just blatantly disregard agreements they have made with their data sources (2009, p. 34).

When social media platforms are utilized in addition to public records, the amount of available PII can increase exponentially, to include valuable details such as comprehensive employment and educational histories; extended family members, close friends and other social groups; pattern of life information such as daily schedules, routes traveled, and favored retail, dining, recreation, and vacation locations; hobbies and interests; and photographic records of an individual, their family, their residence, and other personal details.

Every bit of information that is discoverable regarding a particular individual can then be used to fuel social engineering attempts to gain additional information. Even those social media users who take advantage of available security settings may be more vulnerable than they think. Facebook, for example, offers users the ability to

restrict their timeline from public view; however, even in the absence of the daily updates often provided on a timeline, information useful for social engineering can still be gleaned from a "secured" profile. While a stalker may not be able to view a woman's posts and photographs, he could still obtain crucial details from the often unprotected "About" and "Likes" sections, including schools attended, recreational interests, and local venues frequented.

For example, it would be trivial for someone to use public records to identify a recently divorced, and likely emotionally vulnerable, woman, review her social media, then show up at her favorite local watering hole wearing a t-shirt from her alma matter, and strike up a conversation about the sporting event that she is there to watch on television.

Information Sharing Culture

Information oversharing has become common practice in the 21st century. Social media is an integral part of American culture, with many people checking social media at least daily. According to the Pew Research Center, over three quarters of Facebook users, over half of Instagram users, and nearly half of Twitter users are on the respective sites daily. Over half of Facebook users are on the site multiple times every day (Greenwood, Perrin & Duggan, 2016). We are living in a time where a sizable portion of the population feels the need to regularly broadcast even the most mundane details of their daily lives, and in doing so, are freely giving away valuable pieces of personal information which may be used by criminals in ways the author does not anticipate.

Increased Use of Mobile Applications

Sixty-six percent of the world's population is using mobile phones, and the twelve-month period between January 2016 and January 2017 saw a 30% increase in the number of active mobile social media users (Kemp, 2017). This volume of use and recent increase is significant for several reasons. Mobile social media use means mobile uploads, check-ins, and geotagged posts and photos. In addition to giving away all of the information traditionally associated with desktop use of social media platforms, mobile users are broadcasting their exact locations, and doing so in real time. Numerous studies in recent years have demonstrated various network-based geolocation inference techniques (Jurgens, Finnethy, McCorriston, Xu, & Ruths, 2015). Even if geolocation information is not available for a particular social media user, there are at least nine different methods that could be used to infer that individual's location based on available location data for others within that individual's social networks (Jurgens, Finnethy, McCorriston, Xu, & Ruths, 2015).

Mobile phones now house an inordinate amount of sensitive data. Sensitive data that may be compromised when the phone is lost or stolen, data is intercepted through Wi-Fi sniffing or rogue wireless access points, or taken via malware attack (Jain & Shanbhag, 2012). This sensitive information does not have to be stolen to be used for criminal purposes, in many cases it is simply handed over by the user. The use of any one of the millions of Smartphone apps available almost guarantees that the user is giving away valuable personal information, data that is often entirely unrelated to the operation of the app itself. Location, contacts lists, and media files such as photographs are just a few examples of the many types of information commonly collected by apps.

While many of these apps offer convenience, this convenience comes with the cost of having service providers and random app owners continuously track your every move (Williams & Chi, 2015).

Location-based services create privacy and security vulnerabilities not only in relation to location information, but also in the areas of identity and behavior. The places the user visits, the timing and frequency of those visits, and the presence of others in the area can all provide significant insights into an individual's life including such details as religion, political affiliation, sexual orientation, and medical status (Damiani, 2014). While the average street criminal may not be harvesting location and other information using nefarious apps, organized crime does have access to the resources and expertise required to develop apps specifically for the purpose of collecting information which could subsequently be used to inform criminal activities.

Public Lack of Awareness

Although little research has been done in the area of physical risks associated with the disclosure of PII, research related to privacy and the public's concern regarding the use of mobile apps reveals that the public's privacy expectations and knowledge of the data collection practices from mobile applications are unclear. In "Putting mobile application privacy in context: An empirical study of user privacy expectations for mobile devices, Martin and Shilton conclude:

> Users expect particular data types, such as location and accelerometer data, to be used in the contexts of navigation and weather applications, but they do not expect this data to be used for targeting of advertisements. Users do, however,

> expect keyword harvesting to improve targeting of advertising. And they do not expect contact and image information to be harvested in any context (2016, p. 212).

This research suggests that when it comes to matters of convenience, a significant portion of the public is largely unconcerned with the collection of key pieces of critical personal information from their mobile devices.

Please Rob Me is a site that debuted in 2010, providing detailed location information on individuals obtained from social media sites such as Twitter and Foursquare. The mission statement of the site, which is entirely focused on raising awareness regarding social media safety, begins: “The danger is publicly telling people where you are. This is because it leaves one place you’re definitely not…home” (Siegler, 2010, para 6). Following the launch of the site, a string of over 50 burglaries occurred in New Hampshire. While the site is no longer re-posting location information obtained from social media, it still exists and provides information regarding social media safety, with the added disclaimer that “Our intention is not, and never has been, to have people burgled” (Raising, n.d.). Some believe it was an extraordinarily relevant demonstration of the dangers of social media, while others refuse to see the risks. A review of comments on the aforementioned Siegler article related to this website revealed the views of many skeptics, with comments such as “Has anyone actually ever been robbed due to foursquare or twitter?” “Chill out, people.” and “Surely as long as you don’t broadcast your home address, it doesn’t matter if people don’t know your there?” This last comment appears to be from someone who has not spent much time

with Google, as home address is one of the most accessible pieces of personal information available on the Internet.

Specific Cases and Patterns of Crime Informed by Social Media

In an attempt to establish patterns related to physical crimes informed by social media, research was conducted seeking relevant media articles. These crimes are of particular interest, as the majority of social media content is self-published, and is therefore the source of publicly available PII for which individuals have the most control over, and the best opportunity to take appropriate precautions to avoid victimization.

Research of news reports, utilizing the search engine Google, was conducted on the following twenty-one queries, total search results noted in parenthesis following each query: Facebook stalker (3.24 million), Instagram stalker (371,000), Tinder stalker (5,610), Facebook robbery (4.42 million), Instagram robbery (1.87 million), Tinder robbery (16,300), Facebook burglary (38.8 million), Instagram burglary (207,000), Tinder burglary (3,700), Facebook rape (5.33 million), Instagram rape (8.11 million), Tinder rape (55,300), Facebook abducted (2.87 million), Instagram abducted (294,000), Tinder abducted (3,520), Facebook murder (115 million), Instagram murder (6.95 million), Tinder murder (61,000), Facebook human trafficking (3.17 million), Instagram human trafficking (124,000), and Tinder human trafficking (5,360). In the interest of obtaining comprehensive results, all queries were entered without quotation marks, causing the Google search engine to interpret the queries as "and statements," i.e. the query *Facebook robbery* would be interpreted by Google as *Facebook AND robbery,* thus providing results for any news articles that contain both words. As is the case with any search methodology, there are associated advantages and limitations. The advantage of using "and statements" is that the query *Facebook robbery* would return articles such as "Violent robbery occurs in Rockingham after woman posts photos to

Facebook," which would not be returned had the query been entered in quotation marks as "Facebook robbery." Limitations of this methodology included a large number of false positives that had to be eliminated from consideration, such as articles concerning robberies that had nothing to do with Facebook, but in which Facebook is mentioned, i.e. "According to LAPD's Facebook page, this is the third robbery to have occurred in the Elm Street neighborhood this week."

Due to time constraints associated with this project, only the first 100 results of each of the aforementioned 21 queries were reviewed. Out of the 2,100 total results reviewed, research uncovered 157 reports related to 111 unique incidents or strings of incidents. Some of the strings of incidents represent a significant number of victims, such as a spate of eighteen Denver-area rapes linked to Tinder, or one man in the UK who is currently imprisoned for rape and blackmailing some 100 children into committing sexual acts (Halsne & Koeberl, 2016; Donald, 2017).

The majority of these incidents fall into one or more of eleven categories. These categories include five adverse outcomes from meeting an alleged perpetrator for dating purposes: (1) robbery, armed robbery or theft (2) sexual assault and/or rape, (3) abduction or attempted enslavement, (4) assault, and (5) murder; and six other categories: (6) robbery or armed robbery after the victim agreed to meet the alleged perpetrator for exchange of goods, (7) burglary/home invasion or armed robbery after the victim posted photos to social media, (8) human trafficking/sex trafficking, (9) child pornography and web cam sex trafficking (WCST), (10) men who were accused of rape and blackmailed or acquitted at trial (possibly set up by "victim"), and (11) stalking/cyberstalking/harassment.

A summary of select incidents from each category follows. It should be noted that many of the aforementioned 111 unique incidents or strings of incidents involved two or more crimes (sexual assault and abduction, robbery and assault, etc.), and strings of connected incidents have been broken down and accounted for as individual occurrences, therefor the sum of figures listed as "Total Occurrences" in the following crime descriptions exceeds 111.

1. Robbery, armed robbery or theft after the victim agreed to meet the alleged perpetrator for dating purposes

Total Occurrences: 56

Many, but not all, of these incidents involve direct confrontation. Some criminals showed more creativity and forethought than simply shoving a gun in someone's face and demanding their wallet. In response to an AskReddit thread "What is your Tinder horror story?" one individual recounted the story of a Tinder date in which the female, upon walking through the door to a motel room, indicated that she left her purse in the car. Her date tossed her the keys to his car so that she could go retrieve her purse. She never came back, and when the man went looking for her he discovered, much to his dismay, that his car was gone (Gander, 2016).

Incident Example 1

In November 2016, two Vancouver, WA men were robbed at gunpoint in separate, but connected incidents occurring in the parking lot of an elementary school, where they had arranged to meet a woman for a date. Much to their surprise, upon arrival to the school, the men were not met by the 17 to 23-year-old woman they

expected, they were instead overtaken by four or five men wielding firearms. One of the victims had arranged his date through Meetme.com, and upon arriving at the planned meeting location, was robbed of all his money. The other victim was relieved of his vehicle when the group of men showed up at the same school, where the man agreed to meet his date from Tinder. News reports indicate that police suspect a third robbery may be connected to the first two incidents (2 men, n.d.; Becker, 2016).

It is important to note that one of these incidents occurred at 1:30 am, but the victim waited until the following afternoon to report the crime, citing embarrassment. Although there is no shortage of such crimes being reported, there is no way of knowing how many other similar incidents have gone unreported due to victims who feel embarrassed that they were duped.

Incident Example 2

The Omaha Police Department reported eight incidents of armed robbery (one unsuccessful), occurring over a ten-day period in September 2017. In all eight incidents, the male victims thought they had arranged dates with females through Tinder or Plenty Of Fish, only to be greeted by two or three armed gunmen upon arrival at the arranged meeting location. One victim recounts sharing numerous flirtatious messages with a woman on Plenty of Fish, prior to agreeing to meet her at her home between 2 and 3 a.m. None of the victims were harmed, but the gunmen took phones, cash, debit cards, and jewelry. Omaha police remarked that social media has "become an avenue for robberies," and that the local area had seen a large number of incidents within a short timeframe (Klecker, 2017, para 11; Omaha, 2017, Shapiro, n.d.).

2. Sexual assault and/or rape after the victim agreed to meet the alleged perpetrator for dating purposes

Total Occurrences: 56

While the overwhelming majority of victims in dating robberies are male, virtually all of the sexual assault or rape victims are female. Nearly two-thirds of the 56 incidents identified as part of this project involved Tinder. The UK's National Crime Agency (NCA) reported that the number of rapes linked to online dating increased by more than 450% between 2009 and 2014 (Khan, 2016). In 2016, Oslo Police spokeswoman Kari-Janne Lid said "We began seeing a significant increase last year in the category that includes rapes after initial contact was made on Tinder or other dating sites." (Norway, 2016). Circumstances surrounding dating-app sexual assaults and rapes seem to suggest that different expectations may exist between males and females regarding the intended use of Tinder. Males seem to approach Tinder "dates" with the expectation of a hook-up whereas some females appear to be treating the app as more of a matchmaking service, expecting to find a relationship as opposed to a one-night-stand. In response to an increase in dating app related crimes, Detective Chief Inspector Mark Chicken of the Gloucestershire Police reminded the public that "Just because you have been swapping flirtatious messages it doesn't mean when you do meet up that sex is on the cards." (Norris, 2017).

Incident Example 1

Samuel H. Butler, 22, of St. George, Utah is accused of having raped a Dixie State University student he met on Tinder in January 2017. Multiple news reports

indicate that Butler and the victim shared flirtatious messages via Tinder, and that Butler told the victim he wanted to "get laid," and proposed that they go stargazing on their first date. The victim indicated that she did not want to have sex, but she agreed to meet him for coffee. When Butler picked the victim up, instead of driving to the coffee shop, he allegedly drove the victim to his apartment where he raped her. Following an investigation spanning multiple weeks, Dixie State University police discovered that Butler was accused of forcing himself upon other women under similar circumstances in at least three other Utah jurisdictions, and interviews revealed that Butler's modus operandi involved meeting female college students online (Havens, 2017; Ramseth, 2017; Bolerjack, n.d.).

Incident Example 2

In October 2014, a New Zealand woman was gang raped during a Tinder date she arranged while in Australia for a business trip. After meeting her date at a restaurant, they proceeded to a bar where several of her date's friends later arrived. The victim reported becoming disoriented while at the bar, at which point she was taken to another location and raped by at least three men, according to Sydney sex crime detectives (Partridge, 2014).

3. Abduction or attempted enslavement after the victim agreed to meet the alleged perpetrator for dating purposes

Total Occurrences: 4

Perceptions of risk related to dating vary. Following news reports of local Tinder-related crimes, a University of Georgia student commented, "You make that decision to

meet somebody from Tinder, and I think that if that meeting is in a safe place, there shouldn't be any problems" (Vanden Heuvel, 2016). While meeting in a safe place is definitely a good practice, that will not help in all situations, as demonstrated by the case of Shane Steven Allen, who abducted a woman on their second date, following what appeared, as described in court documents, to be an acceptable first date (Tulp, 2016).

Although most dating related crimes occur during an in-person meeting, some occur when one party seeks out another without prior agreement to meet. One of the four abduction incidents listed above occurred after a woman ended an online Facebook "relationship" before she ever met her attacker in person. The jilted man then drove across the country intent on abducting the woman, taking her back to Georgia, impregnating her, and making her his bride.

Incident Example 1

In May 2016, a University of Kansas student was allegedly beaten during her second date with Shane Steven Allen, a 30-year-old man whom the sorority sister had met through Tinder. According to court documents, Allen had taken the victim to his home, in the company of two of his friends. After the others departed, Allen accused the victim of flirting with his friends, and proceeded to punch her in the face and take her to the ground. He subsequently held her captive in his trailer and beat her several more times over the course of six days, including choking her unconscious when she attempted to leave. University of Kansas students interviewed following the incident were shocked, providing comments such as "I was absolutely flabbergasted that had happened" and "It made me think about the fact that it is a common occurrence in

college…It really opened my eyes to the (dangers of the) whole hookup culture thing" (Tulp, 2016; Bult, 2016).

Incident Example 2

Following the demise of a relationship begun on Twitter, which included one in-person meeting, Robin Gomes broke into a woman's Bristol, England, house with a carefully conceived plan to abduct her and make her his sex slave. Following a one-night-stand, the woman indicated that she did not intend for the relationship to go any further. Gomes subsequently tracked down her home address via the Internet, and showed up at her rural home to declare his love to her. He made several repeat unwelcome appearances, and ultimately broke into her house, claiming that the woman had no right to deny his sexual advances. The judge who sentenced Gomes to ten years in prison stated "You've said this woman was your 'c**** bucket', nothing more than a hole to have sex with…You wanted to chain and cage her. You admitted you would have raped her if necessary…Yours was a planned offence with sadistic excitement of inflicting fear into your victim. You are dangerous in that you represent a risk of serious harm to the public in the future." (Baynes, 2016).

4. Assault after the victim agreed to meet the alleged perpetrator for dating purposes

Total Occurrences: 10

Although most of the assaults identified for this project occurred in conjunction with a robbery, this may change as more personal information becomes readily available. Social media could become an even more useful resource than it already is

for individuals looking to commit hate crimes. In an effort to become more inclusive, Tinder announced 37 new gender options available for US-based users in November of 2016. The expanded offerings were made available to users in Germany, Spain, and France in June of 2017. The specificity of this information could aid in one's efforts to target a specific group of individuals to assault, or as is discussed in the next section, murder (Lang, 2016; Clarke-Billings, 2016; Introducing, 2016).

Incident Example 1

In late 2015, two Minnesota men were assaulted in related incidents. According to a *Pioneer Press* news report, "The M.O. was the same both times: Find a stranger on social media, make a date and have a friend show up a bit later with a gun" (Vezner, 2017, para 1). The first man was robbed of $160 in cash and shot in the leg during a date with a woman he met through Facebook. The woman had claimed to be new to the area, and met the victim for drinks at his home. Shortly after the woman arrived, two armed men walked into his apartment and demanded money. A week later the same woman arranged a date with another man through Instagram. That man picked the woman up in his BMW, and shortly thereafter a man ran up to the vehicle, and tased and pistol whipped the victim through the window (Vezner, 2017).

Incident Example 2

In July 2016, a California woman was beaten about the head so severely by a man she met on Instagram that her brain swelled. Following a night on the town, the man, James Baker, took the victim to a Los Angeles hotel where he savagely beat her and left her for dead, taking with him her car and cell phone. Police utilized the Find My

iPhone app to locate the victim's cell phone and track the man down at another area hotel. It was later discovered that Baker had multiple prior convictions in other states, and was on bail for credit card fraud. According to KTLA 5 Los Angeles, the victim is quoted as stating "I wouldn't want anybody to go and meet up with anybody that they don't know. Please don't ever do that…You have to value your life" (Mcdade & Kurzweil, 2017, para 17). The victim also commented that she felt comfortable meeting Baker in person because "He didn't really look like a creep from his pictures. He looked like he had it going on" (Mcdade & Kurzweil, 2017, para 3).

An iOS dating app released in 2017, Gatsby, performs criminal record and sex offender searches, supposedly blocking users who have prior convictions. While this app may be effective in certain situations, and quite possibly could have prevented the incident involving convicted criminal James Baker, there will be limitations. Not all jurisdictions make criminal records available to these types of services, the app cannot protect users from individuals who have committed crimes and not been caught, information on recently committed crimes may not be available, users may register under false identities, and the app will be of no use in the case of first-time criminals. Provided that the app takes hold, research would have to be conducted to determine how effective the app actually is, and whether or not it provides users a false sense of security (Alba, 2017).

5. Murder after the victim agreed to meet the alleged perpetrator for dating purposes

Total Occurrences: 13

Murder connected to social media does not appear to happen nearly as often as theft and assault, but it has happened enough to be worth mentioning. Some of the murders have been the result of robberies gone bad, some pure acts of rage, and yet others seemingly premeditated acts carried out by methodical killers such as the case of Jason Marshall, described below, and the case of Emmanuel Delani Valdez Bocangegra, who was arrested in Mexico City for murdering his Tinder date and dissolving her body in acid (Leighton, 2016).

Incident Example 1

Richard Nyakina Ogoko, a 26-year-old Kenyan, is accused of murdering 23-year-old Lydia Nyaboke on their first date in Nairobi on 23 July 2017. According to *Nairobi News* reports, the couple had met through Facebook, and had communicated via telephone on several occasions before meeting to have a picnic for their first date. Reports indicate that the suspect initially contacted the victim, indicating that they had much in common, as they were from the same Kisii village. It was noted that Ogoko's Facebook account displayed a profile photograph of someone else, and that he had a disproportionately high number of female friends. Ogoko confessed to police that he suffocated the victim after striking her on the head, and ultimately used the victim's clothes to strangle her. Ogoko is also facing rape charges stemming from an incident two years earlier (Facebook, 2017; Pending, 2017).

Incident Example 2

In 2013, Jason Marshall, 28, a former male escort from London, went on an international rampage, using the dating app Badoo to lure multiple men and

subsequently kill them. According to court records, Marshall had a habit of dressing in various uniforms, and was impersonating a police officer when he gagged and suffocated Peter Fasoli, then set Fasoli's London home on fire. Marshall then stole Fasoli's credit cards and used them to fund a trip to Rome, where he killed Vincenzo Iale. He then stole Iale's vehicle and credit card, and a week later arranged another Badoo date with Umberto Gismondi, who he also attempted to murder (Eustachewich, 2017).

6. Robbery or armed robbery after the victim agreed to meet the alleged perpetrator for exchange of goods

Total Occurrences: 19

These incidents seem to happen more often at night. In some cases, the perpetrators advertise items for sale, which ensures that their victims bring cash. In other incidents, perpetrators act as interested in buyers, then steal the item being sold.

Incident Example 1

On 25 June 2017, a Chicago man was robbed at gunpoint after traveling to Milwaukee to purchase a moped that was advertised on Facebook Marketplace. The victim had been in contact with the seller for several days, and admitted to feeling safe because the transaction was initiated through Facebook. After the victim gave the suspect a ride to retrieve the moped's title, the suspect returned to the vehicle with a gun, and demanded that the victim hand over the cash he had brought to purchase the moped. The incident was recorded on the victim's dashcam, and the suspect was later identified (Sears, 2017).

Incident Example 2

In June 2016, Kameron Dominic Alston, of Chicago, contacted another Illinois man through Facebook to arrange the purchase of marijuana. When the two met in a neighborhood in which Alston claimed to reside, Alston grabbed the marijuana as well as the seller's arm, pulling the man half way into his vehicle through the window, then drove off with the victim's head and torso inside the vehicle and his legs hanging out the window. Alston hit a parked car, at which point the victim was tossed into the street, and Alston made off with the marijuana. As a result of the violent robbery, the victim was in a coma for over a month, is paraplegic, and has no use of his hands (Briscoe, 2017).

7. Burglary/home invasion or armed robbery after the victim posted photos to social media

Total Occurrences: 39

Several of these burglary incidents occurred within the homes of individuals who posted vacation pictures in real time. UK-based Co-op Insurance conducted a survey of 2,000 people regarding their basic security practices. Twenty percent of respondents admitted to sharing vacation photos while they were still on vacation; other sources have placed the number as high as 58% (Smithers, 2017; Culley, 2017). Noel "Razor" Smith, a former bank robber who served 32 years in prison for some 200 robberies, said "Bragging about your holidays is an absolute no-no. It's just saying 'come and burgle my house'. Organised gangs are having a field day." (Smithers, 2017). According to the home security provider ADT, 78% of burglars are using social media to target

homes, and some experts suggest that negligence in social media posting habits amounts to failure to exercise “reasonable care,” a condition which could invalidate insurance policies (Christie, 2017). Sgt. Kelvin Courtney of Ireland’s Garda National Crime Prevention Unit perhaps summed it up best when he stated “People need to realise that whatever they are putting up online; they may as well write it on a piece of paper and stick it to the front of their house” (Lally, 2016).

Incident Example 1

In February 2017, three armed men broke into a Philadelphia home to steal items they had seen posted on a 19-year-old resident’s Instagram account, including Rolex watches and other valuable jewelry. Five male victims between the ages of 17 and 19 were in the residence at the time of the robbery, and the thieves made off with cellphones, a Rolex watch, and multiple gold chains (Johnson, 2015).

Incident Example 2

A California man, Arturo Galvan, received an eight-year prison sentence after breaking into the homes of 33 female college students to steal their underwear and valuables totaling over $250,000. The married father of three committed the crimes between 2014 and 2015, after locating victims’ homes by using geolocation information from photos the victims posted on Instagram. The exact circumstances of these crimes are unclear. Some reports indicate that the suspect targeted women he had seen in public places, tracked down their social media accounts, and then pulled geolocation information embedded in photographs, while other reports make no mention of in-person encounters between Galvan and the victims prior to the commission of the

crimes. Additionally, one report indicates that Galvan pulled metadata from both Instagram and Facebook photos, however, as a matter of practice, Facebook wipes exchangeable image file format (EXIF) and other metadata from photographs upon upload (Ludwig, 2016; Blake, 2016).

8. Human trafficking/sex trafficking

Total Occurrences: 12

The incidents outlined in this report are a small sample of what is currently taking place in the realm of human trafficking. Spotlight, a web scraping tool which was developed by Google engineers in cooperation with anti-trafficking organizations, uncovered 6,000 victims of sex trafficking advertised on the online commercial sex market, and 2,000 traffickers, in a single year (Molinari, 2017). As of November 3, 2017, the Spotlight website boasted the identification of over 6,625 victims, sourced from the 100,000 new escort ads that are posted online every day (Spotlight, n.d.).

Although many trafficking incidents occur when the victims agree to meet in person; it is the information a victim posts online which leads to them being targeted in the first place. Criminals are going for easy marks, those who are most vulnerable, posting their thoughts, feelings, and desires online for the world to see. An agent from the Fort Wayne, Indiana FBI office remarked “If you put on there everything your parents don’t understand, how easy is it for me to pop up online and say it doesn’t have to be like that. You’ll get your hair done. You’ll get your nails done. You’ll eat three times a day. I’ll give you a warm place to stay, nice hotels.” (Traffickers, 2017). While not all of the victims identified by Spotlight were victimized as a result of their own social

media use, the overall human trafficking figures are startling, and there is evidence that many of the sex traffickers are identifying their victims and making initial contact through social media. As former Congresswoman Susan Molinari recently pointed out, "Technology's role in human trafficking cannot be ignored." (Molinari, 2017, para 8).

Incident Example 1

According to detectives in the Human Exploitation and Tracking Unit of the Mesa Police Department in Arizona, Oshay Small and Cornelius Wells used Facebook to initiate contact with two 15-year old girls, and convinced them to leave home. The girls were then advertised on the Internet, and sexually exploited for profit. Upon investigation, police learned that two women and one additional girl were also being exploited. Small and Wells were taken into custody following a five-month long investigation (Gundran, 2017).

Incident Example 2

An Atlanta man is under investigation by the FBI for alleged human trafficking after one of his victims called 911 in early 2017. Kenndric Roberts was living in a rented mansion with eight women he referred to as his "Diamond Kitties." Roberts had utilized dating sites and other social media platforms to contact vulnerable women, offer them jobs at his company, which he stated represented models and athletes, and lure them to Georgia. Once the women arrived at the Sandy Springs house, which Roberts routinely patrolled with an AK-47, he forced them to work in strip clubs, and threatened to kill anyone who tried to leave (Noll, 2017; Carlson, 2017).

9. Child pornography/web cam sex trafficking (WCST)

Total Occurrences: 101

This category of crime generally involves no physical interaction between the perpetrators and victims; however, the traumatic psychological impacts to victims are profound and enduring. Both the Federal Bureau of Investigation and the United Nations have been quoted as estimating the number of predators who are on the Internet at any given moment to be 750,000 (Webcam, 2013). A group of researchers from Terre des Hommes Netherlands spent ten weeks in 19 public chat rooms, posing as young Filipino girls to see how many predators would seek them out for WCST purposes. During that time, they were contacted by 20,172 predators from 71 countries, 1,000 of whom the research team were able to positively identify (Webcam, 2013). According to Terre des Hommes, contact is usually first made through online dating sites, social media platforms, public chat rooms, or cybersex dens. Although WCST seems to be more of a problem in developing nations, there is no way of knowing how many US children are being exploited in this manner, and many of the criminals engaged in these activities hail from developed countries. It is an international problem that has not received enough attention, as the number of predators convicted to date is a shockingly low six (Webcam, 2013).

Incident Example 1

British pedophile Paul Leighton utilized some 30 or 40 false personas on Facebook to pose as a minor and befriend teenagers from Australia, Canada, and the US, under aliases such as June Clarke, Laya Anderson, and Emma Sanderson. After establishing relationships with his victims, Leighton convinced the teens to send him sexually explicit photographs of themselves. He then blackmailed the teens, forcing

them into sex acts by threatening to disseminate their naked photographs if they did not do as he instructed. Several of the minors were coerced into committing crimes against others to appease Leighton, including several cases of children engaging in sexual acts with their siblings, and a 14-year-old Florida boy who was forced to rape his one-year-old niece. Despite the fact that he was not physically present for the commission of the crimes, Leighton was charged with rape and sentenced to 16 years in prison. Authorities believe it likely that Leighton had many more as of yet unidentified victims (Donald, 2017).

Incident Example 2

A 21-year old man from the Philippines was arrested in July 2017 after he contacted a minor through Facebook under an assumed name, and convinced her that he would pay her to send him nude photos and videos. Once the victim sent the photos and videos, the man refused to pay, and informed her that he planned to disseminate the compromising images unless she had sex with him. In an effort to avoid public embarrassment and shame, the victim agreed to meet the man, at which point he allegedly raped her, and then demanded money. The victim gave the man money, then sought assistance from law enforcement. Upon the man's arrest by the Philippine National Police Anti-cybercrime Group, authorities located nude photographs of several other young girls on his phone (Legaspi, 2017).

10. Men who were accused of rape and blackmailed or acquitted at trial (possibly set up by "victim")

Total Occurrences: 3

While the initial research for this project, largely conducted in September 2017, did not reveal many cases of false accusations, specific searches were not made seeking such incidents. This was added as a category when results from other targeted searches uncovered multiple incidents. A simple search of the term “Plenty Of Fish,” aimed at obtaining a description of the website, returned several articles related to UK resident Samantha Murray-Evans, who was recently sentenced to 27 months in prison for falsely accusing her Plenty Of Fish date of rape (Hardy, 2017). It is likely that a targeted search seeking information related to these cases would uncover additional incidents, whether the result of malicious intent or revenge for relationships gone south.

Incident Example 1

Following the demise of a relationship that was first initiated through Tinder, a woman allegedly harassed a Houston man on a daily basis, sending him unwelcome text messages, and posting derogatory comments about him on various websites and social media platforms, calling him a “creepy butcher marine farmer” (Brown, 2017, para 5). The woman accused him of rape, attempted to blackmail him for $10,000, and when he refused to pay, she went public with her accusations. The man, Joseph Lazarus, is now suing the woman for blackmail and libel, after he was fired from his job when his boss saw posts claiming that Lazarus would “rape fat chicks just to amuse his friends” (Brown, 2017, para 9).

Incident Example 2

A 21-year-old British rugby player was accused of raping a woman he met on Tinder with “fear and force” (Evans, 2016, para 1). The man was subsequently cleared

of all charges by the Newcastle Crown Court in August 2016, when a jury determined that the woman had consented to intercourse (Evans, 2016).

11. Stalking/cyberstalking/harassment

Total Occurrences: 13

The number of tools available to stalkers is growing at a startling pace. Numerous recent media articles cite ways in which stalkers can utilize social media for purposes other than those for which the platforms were originally intended. In 2015, Tinder began enabling users to link their Instagram accounts to their Tinder accounts, giving rise to the practice of "Tindstagramming," whereby failed Tinder matches can access the subjects of their desire through Instagram. In addition to providing the opportunity to direct message individuals through Instagram and harass them that way, the direct link from Tinder to Instagram often provides an individual's full name, which in combination with general location information from Tinder, can easily enable a stalker to locate someone's home address (Tindstagramming, 2017).

Facebook's "People You May Know" section can also be abused by stalkers to gain access to their victims. Facebook friends lists are seen by some as a sign of popularity and social standing – the more friends one has, the better. Individuals who subscribe to this method of thinking may send friend requests to anyone and everyone who Facebook suggests as People You May Know in an attempt to bolster their friends count, assuming that the platform is suggesting friends of friends, even if they have no idea who the people they are friending really are. The problem is, Facebook algorithms do not merely suggest friends of friends or individuals with common interests as People

You May Know. The suggestions also include individuals who have spent a significant amount of time viewing your profile. It is this functionality that can prompt individuals to grant unknown stalkers access to additional information, and an entry point into their life. Noted anthropologists such as Robin Dunbar suggest that the number of social relationships a person can effectively maintain numbers in the low hundreds; yet many people find it perfectly acceptable to increase their circle on social media to the thousands, opening themselves up to exploitation by many individuals whom they really do not know (Silver, 2016).

Especially concerning is the new app, Dating.ai, dubbed by *Forbes* contributor Janet Burns as "The perfect app for superfans, stalkers, and serial killers." (Burns, 2017). Dating.ai enables a user to upload a photograph of someone they find appealing. The app will then utilize facial recognition to scour other platforms such as Plenty Of Fish, OkCupid, and Tinder for profiles of individuals resembling the person in the uploaded photograph. Searches can be limited by age, gender, and area code, and uploaded photographs can come from anywhere (Burns, 2017). Match.com CEO Mandy Ginsberg has remarked that "Match.com is no different than society. If you go out to a bar and meet someone that you don't know, you should be careful." (Werber, 2017). While Ginsberg's analogy may be true to an extent when viewing certain dating apps in isolation, services such as Dating.ai take more "traditional" apps and exponentially increase the creep factor.

Dating.ai is the perfect tool for stalkers. When in need of a new victim, a stalker just has to lurk at a coffee shop until someone of interest walks in. After identifying the desired target, the stalker surreptitiously takes a picture with his cell phone, which can

be accomplished with relative ease while he is pretending to text someone. He then uploads the photo to Dating.ai, enters a local zip code, and with any luck, he will be provided a direct link to the Tinder account of the woman standing in line waiting for her latte. According to Tinder founder Sean Rad, this is only the beginning. Rad foresees a future where individuals may be able to access someone's dating profile simply by pointing a phone at them (Werber, 2017).

Although all incidents of cyberstalking will most certainly be unsettling for any victim, some can be especially troubling, causing significant emotional distress even in the absence of physical contact. Notorious cyberstalker Jason Christopher Hughes has been accused of ruining the lives of multiple victims, including one woman he met through social media, to whom he sent an email in September 2015, with the following instructions on "How to Make Your Own Pet Owl.":

> Take one human. smash the arms, legs knees with a sledge hammer. bend the twisted limbs around a perch in a large iron cage. bind the limbs so they grow into place. insert a PEG tube directly into the stomach for liquid feeding. nasal feeding gets in the way of the next stage. bust out all off the teeth. remove the tongue. blinding is a nice option at this stage, but you might want to wait on that to set the unfinished owl in front of a large mirror for some weeks. cut the cheeks midline, break the lower jaw and collapse the pallet. at this point a stomach tube might be left with the facial remnants formed into a "beak." keep a bucket underneath your new Owl to catch wastes. have fun poking your Owl with thin, sharp bamboo slivers. keep the owl on constant multiple antibiotics, and switch

these up so skin sepsis doesn't set in (Hensley, Keshner, & Annese, 2017, para 7).

This is but one example of the many disturbing and threatening unwanted communications women received from Hughes. One would be hard pressed to find an individual who would not be terrified and potentially permanently scarred by the receipt of such a communication.

Incident Example 1

Brandon Lapp, of Lancaster, Pennsylvania, pled guilty to harassment after he utilized social media to target a woman he never met, decided that he was in love with her, and began harassing her boyfriend, of whom Lapp was extremely jealous. Lapp created fake Facebook pages in the boyfriend's name, using stolen photographs, and made it look as though the victim was gay. Lapp also placed ads seeking male prostitutes on backpage.com, which resulted in the victim receiving at least 30 phone calls from prostitutes offering their services within a single day. Other activities including anonymous phone calls, harassing the victim's father, and ordering pizzas delivered to the victim's workplace (Miller, 2017).

Incident Example 2

In late 2016, Australian Paul Lambert stabbed a woman 11 times and doused her in gasoline following the end of a brief relationship that began on Tinder. Lambert was shot dead by police following a 100-mile chase after the incident. At least four women have come forth indicating that they were previously stalked or harassed by Lambert. Reports from these women indicate that upon meeting Lambert online, he would work

hard to convince them to come to his apartment, as opposed to meeting for the first time in a public place. Following the heinous attack, one of Lambert's other stalking victims, with whom he had communicated via SnapChat, remarked "It took my breath away. I mean being creepy is one thing, being a psycho is another and that's clearly what he was… You never imagine that someone you're talking to could be actually capable of hurting someone like that. It's disgusting" (White & Cleary, 2017, para 14; Awford, 2017).

Other incidents

Several additional incidents occurred which do not fit into the aforementioned general categories. These incidents include four Kenyan women who were gang raped when they agreed to meet potential employers who had contacted them via Facebook, and the assault of a teenager after multiple individuals took issue with something the teen had posted on Facebook, tracked down her home address, forced their way into the family home, and assaulted the teen and her mother (Alarm, 2017; Jechow & Rangel, 2017).

It should be noted that information uncovered as part of the limited scope of research conducted for this project is merely the tip of the proverbial iceberg. Significant limitations of this research include time period covered (nearly all of the incidents examined occurred between 2015 and 2017); the utilization of a single U.S.-based search engine; the limited number of searches conducted, focusing only on seven crimes in conjunction with three social media platforms; and the fact that for the searches that were conducted, not all documents were reviewed. Additionally, it is likely

that not all physical crimes informed by social media or other sources of PII are reported as such.

Specific Cases and Patterns of Crime Informed by Other Publicly Available Sources

Although this report focuses mainly on crimes informed by social media, there are plenty of other examples of crimes being informed by other publicly available sources of identity information. Examples of this include burglars who use obituaries to identify vacant homes, and stalkers who use public records to locate their victims.

While the availability of public records is not new, the accessibility of these records has greatly increased. Instead of having to go to a courthouse, library, or other public institution to conduct manual searches, the Internet provides easy access to a wide variety of records, irrespective of the physical location of the record and the researcher. Additionally, new sources of personal information, such as social media, can be used to guide searches for public records. For example, A Facebook post related to a death may prompt a search for an obituary, a Tweet regarding a college football game may motivate someone to seek educational records, or Instagram photos of a housewarming party may spur research of property records.

Funeral burglaries

Funeral burglaries, crimes in which the perpetrators obtain viewing and funeral information from obituaries, then strike the homes of the deceased or friends and family when they know the homes will be vacant, are nothing new. Criminals have utilized this modus operandi for decades, but access to online obituaries makes the planning effort easier, and enables groups of criminals to attack widespread areas instead of being limited to the information contained in the local newspaper. In 2013, Seattle area police investigator Margaret Ludwig recalls busting a group of criminals “Running an obituary

crime ring so sophisticated and organized, even seasoned investigators were stunned." (Rossen & Davis, 2013). More recently, Indiana State Police issued a warning to the public in the wake of a multi-county string of burglaries which occurred in early 2017 (Burbrink, 2017), and Illinois State Police and Missouri funeral directors issued similar warnings after a rash of burglaries in the St. Louis metro region in May 2017 (Rieck & Landis, 2017).

Stalkers

According to The National Center for Victims of Crime, stalkers frequently obtain information on their victims through public records or online searches (Rossen & Davis, 2013). Although he utilized social media to target at least one of his victims, Jason Christopher Hughes, the aforementioned stalker from Staten Island, NY, also used other publicly available sources to locate victims. According to a criminal complaint filed against Hughes, he located one of his victims, a former fourth grade pen pal from the 1970s, through contact information provided on the website of the school where she was employed in 2015 (Wassef, 2017).

Patterns Observed Within Media Reporting

Local TV news stations provide the majority of reporting related to crimes informed by social media and other publicly available information. Very few national news outlets in the US report on these crimes, although nationwide reporting seems to occur much more frequently within the UK, from outlets such as *The Mirror*, *The Guardian*, *The Daily Mail*, and *The Daily Star*. Research for this project uncovered several articles providing statistics related to these types of crimes, as well as cautionary warnings to UK residents. And yet some within the UK, like former *Wall Street Journal* reporter Cassie Werber, believe that significant gaps remain within UK research and crime reporting (2017).

While it may be true that UK crime reporting with regards to social media connected crimes is less than ideal, at least there is some reporting. The UK Press Association reported a 560% increase in dating app related crimes between 2013 and 2015 (Ng, 2016). Scotland Yard reported a 2,000% increase in dating app related crimes from 2012 to 2016 (Alexander, 2016). No such statistics have been widely reported within the US. Given the number of local US-based news reports identified, it would appear that the lack of widely publicized statistics does not indicate a lack of crime, but instead a lack of reporting.

For those incidents that have been reported within the US, reporting tends to be vague, with many news reports failing to even mention the specific platforms involved, instead reporting that victims were located “through their social media accounts,” or stating that a woman met the man who would later sexually assault her “through a dating app.” And while some headlines are fairly specific, such as “Teenager faces

charges after setting up sneaker robbery on Facebook" and "Tinder bait & switch leads to Fresno armed robbery & auto theft," others obscure the involvement of social media, such as "Cousins linked to murders of two Houston-area men" or "St. George man charged with rape" (Jones, 2017; Hoggard, 2015; Cerullo, 2017; Ramseth, 2017). Not only are reports of incidents not making national headlines, but the local reports often lack sufficient detail to enable readers to take proactive measures in ensuring their own security. It is unclear whether the lack of content is perhaps a result of police trying to keep a close hold on information related to ongoing investigations, or a lack of interest on the part of journalists.

Public Perceptions of Risk

Public Figures as Victims

The crimes detailed in the Specific Cases and Patterns of Crime Informed by Social Media section of this report all have one thing in common; the victims are average, ordinary people. We have seen that the reporting on these crimes is often minimal, and yet these are the victims to whom the majority of the population can relate. The reporting of crimes related to celebrities and other public personas, however, is vastly different.

In the nine months between October 2016 and July 2017, multiple public figures, including Kim Kardashian, Alanis Morissette, John Terry, and Hilary Duff, were the victims of crimes directly related to posts the celebrities had made on Instagram:

- In October of 2016, Kim Kardashian was the victim of an armed robbery when several men broke into the residence where she was staying during Paris Fashion week in the middle of the night, tied her up, and stole over $14 million worth of jewelry. The incident happened shortly after Kardashian posted a photograph of her $4 million engagement ring on Instagram. Following the incident, which resulted in the arrest of sixteen people with mob connections, Kim's sister Khloe indicated that the robbery was God's way of showing the family that they need to be more concerned about security. In defense of her sister, whom some say was partially at fault for the robbery for showing off her valuables, Khloe remarked "I could show you hundreds of people on Instagram who show off wads of cash and diamonds" (Martinez, 2017; Khloe, 2017, para 8).

- In February of 2017, thieves broke into Alanis Morissette's Brentwood, California home and made off with a safe containing $2 million worth of jewelry. In the months leading up to the burglary, Morissette had documented her jewelry collection on Instagram and a blog, including identifying the designer of each piece (French, 2017).
- In early 2017, the home of British soccer player John Terry was burgled while his family was on vacation. Terry had recently posted photographs of the interior of his home on Instagram, and also posted photos of the family's ski trip to the French Alps, providing all the information the criminals needed to effectively target the mansion, and make off with over a half million dollars' worth of valuables (Moore, 2017).
- In July of 2017, Hilary Duff posted a video to Instagram with the caption, "CANADA," letting anyone who was looking, and in particular her 8 million Instagram followers, know that she was on a family vacation. Shortly thereafter burglars broke into Duff's Los Angeles home and reportedly made off with hundreds of thousands of dollars in jewelry (Here's, 2017; Mcallister, 2017).

Unlike the majority of social media related crimes, where reporting is frequently limited to local news outlets, the reporting of these crimes was international, with stories carried by news outlets such as People, The Sun, Vanity Fair, US Magazine, The Atlantic, The Daily Beast, Bravo TV, Allure, Forbes, The Washington Post, The Los Angeles Times, and the NY Times. This broad reporting of celebrity victims leads to the heretofore unaddressed question of how might this influence public perceptions of risk? If people are exposed to a disproportionate amount of news regarding celebrity

incidents as opposed to incidents involving average people, will they think that crimes informed by social media are a problem exclusively for public figures?

Pop Culture References to Crime Informed by Social Media

As seen in recent pop culture references in fictional books and movies, the idea of average people becoming victims of social media related crimes is not entirely unthinkable. The 2017 film *Ingrid Goes West* chronicles young Ingrid Thorburn's move across the country in a desperate bid to befriend her Instagram obsession; Taylor, a Los Angeles woman whom Ingrid believes "has it all." Early scenes in the movie show Ingrid as an inpatient at a mental health facility following an incident where she attacked a bride at her wedding reception because their social media relationship led Ingrid to believe she should have been invited to the wedding. Although Ingrid's mother had recently passed, surely adding stress to her life, the movie seems to suggest that perhaps her mental condition was exacerbated not only by her mother's death, but by Ingrid's obsession with social media, an obsession which enabled constant comparison to others whom she perceived to have more desirable, if not perfect, lives.

The movie also highlights how some people utilize social media so much that they perhaps become desensitized or oblivious to what is really happening in their interactions. Prior to moving to Los Angeles, Ingrid communicated with Taylor online, making comments on Taylor's Instagram posts, to which Taylor would respond. Several scenes, presumably occurring within Ingrid's first few days in California, show her in places Taylor frequents, hoping for a "chance" encounter, of which there end up being several, all informed by personal information Taylor had published via Instagram. Once the two formally meet, Taylor neglects to realize that Ingrid is one of her "Instafans,"

despite the fact that Ingrid used her full, true name in both online and in-person interactions with Taylor.

While Taylor and Ingrid seem to become the best of friends rather quickly, the relationship, which was built upon false pretenses, falls apart nearly as fast as it initially flourished. Towards the end of the movie, Ingrid live streams her attempted suicide, remarking “I’m just tired of trying to make people like me. I’m tired of pretending like, I’m someone I’m not. And I’m tired of being alone” (Spicer, 2017). The scene then jumps to Ingrid in a hospital room, brimming with balloons and flowers. Just as Ingrid had become obsessed with Taylor through her social media presence, hundreds, if not thousands, of individuals around the world had become obsessed with Ingrid.

Although *Ingrid Goes West* was written primarily for entertainment purposes, it is an excellent illustration of how social media influences our social interactions, and how vulnerabilities grow, often unnoticed. We have already seen these vulnerabilities played out in reality. For example, some of the themes in the movie are very similar to the 2016 real-life case of Instagram user diana_alexa following Instagram user gypsea_lust around the world, recreating, with painstaking detail, the latter user’s vacation photographs (Seals, 2016; Morgan & White, 2016). This is but one real-life parallel; the movie provokes numerous questions regarding other ways in which the storyline may be relevant, such as:

- To what extent does social media not only enable crime, but inspire otherwise law-abiding citizens to become criminals as a result of the altered perceptions of reality that are seen online?

- Is the risk of having complete strangers become obsessed with one's life, worth the reward of the ego boost provided by a few thousand followers?
- Does the existence of a carefully curated online persona somehow dehumanize criminals' perceptions of their victims? I.e. for those who do realize just how fake a supposedly perfect life presented through social media can be, do criminals view victims more as a fictional character as opposed to a real human being?

Other references to social media vulnerabilities are seen in Clare Mackintosh's book *I See You.* Mackintosh paints a twisted picture of a pair of criminals who utilize social media and other sources of PII to stalk women on the London subway. After building significant dossiers on their victims, to include minute-by-minute details of their daily commutes and other routines, the criminals then sell the packages of information regarding the victims to those looking for the thrill of a good hunt. Several women go missing, end up sexually assaulted, or murdered (Mackintosh, 2016).

Although the storyline in this book is a bit more far-fetched than that of *Ingrid Goes West*, it also provokes questions, specifically regarding the general public's overall knowledge and utilization of social media privacy settings. In the book, the main character, who is one of the stalking victims, remarks that she had no idea that Facebook even had privacy settings. She had been utilizing the social media platform as a personal diary, and was shocked to discover that her entire timeline was visible to the world. It is interesting to note that the author of this book is British, and the setting is London, while we have seen, as previously discussed in this paper, that reporting of social media-related crimes seems to be more prevalent in the UK than the US. Also of

note is the fact that Mackintosh spent 12 years as a police officer prior to pursuing a writing career, although the impact, if any, that her law enforcement career has had on her fictional storylines is unknown (Bestselling, n.d.).

Conclusion

In response to recent reports that Facebook allowed targeted advertising with offensive terms, Facebook COO Sheryl Sandberg commented, “We never intended or anticipated this functionality being used this way – and that is on us.” (Roose, 2017). There are multiple ways in which social media platforms can, and are, being used for alternate, undesirable purposes. Kevin Roose, of *The New York Times,* has likened these scenarios to the moment Frankenstein’s creator realized that he had created evil, remarking “I had been the author of unalterable evils… and I lived in daily fear lest the monster whom I had created should perpetrate some new wickedness.” (Roose, 2017). Similar sentiments have been shared by others, including former Facebook advertising executive Antonio Garcia Martinez, who said “The reality is that if you’re at the helm of a machine that has two billion screaming, whining humans, it’s basically impossible to predict each and every possible nefarious use case.” (Roose, 2017).

Even as they forge ahead in creating technological solutions to enable people to find each other with ever-increasing ease, most platforms acknowledge, even if indirectly, that there are some serious safety issues with the current state of affairs in the dating app realm. Tinder stresses on their website that users should meet dates in public places, keep a charged cell phone with them at all times, inform friends and family of their planned itinerary, drive to the date location independently to enable a speedy departure if necessary, refrain from consuming alcohol or drugs, and “be aware that bad actors might try to take advantage of you by altering your beverage(s) with synthetic substances.” (Dating, n.d.). And they provide phone numbers for national rape and domestic abuse hotlines.

Even given the limited scope of the research, this paper has identified many important research questions that still need to be addressed. One key finding, supported by admission of social media executives, and with evidence of a multitude of reports of crime informed by social media, is that there is no question that criminals are in fact using social media to aide in the execution of their criminal endeavors. But the true extent of this use is unknown.

One of the biggest challenges facing researchers is the different ways in which various municipalities account for crimes, making any attempts to definitively research trends and crime rates related to social media and other publicly available sources of information onerous. Police departments keep detailed individual crime reports, but far more general overall statistics. For example, you may find that there were 351 assaults reported in Smalltown, USA in 2016, but without reviewing each individual report, you have no idea how many of those crimes involved someone getting punched in the face, someone getting shoved to the ground, or someone being spit upon. Similarly, you may be able to find out how many burglaries occurred in Des Moines in 2015, but it would be much harder to ascertain exactly what methods the criminals used to target homes. General statistics do not reveal if someone's home was broken into after they posted vacation pictures online, or if it occurred after they left the boxes for a PlayStation 4, a stereo, and a 60" TV out on the curb after Christmas.

In order for any accurate conclusions to be drawn regarding trends in social media and PII-related crimes, there needs to be an overall and widespread shift in the way police are accounting for these crimes. And while it currently may be feasible for a researcher to comb through the details of all criminal reports for a specific city, the

results of such research would likely be skewed by geographic and socioeconomic factors limited to the specific area in which the research was conducted, and therefore an inaccurate comparison to what is going on in a larger region such as a particular state or country.

Once the issues surrounding inadequate reporting are resolved, there will still be many questions to answer, such as why does the overall problem seem to be receiving more attention in the UK than in the US? Is it because these types of crimes occur more frequently in the UK, or are the UK media outlets simply ahead of the curve in their reporting? Perhaps the most important questions for future research to address would be whether or not social media and other publicly available identity information have actually caused an increase in certain types of crimes, to what extent social media use may increase one's likelihood of becoming a victim, and what other factors, such as geography, may influence crime rates.

Appendix

Event	Year*	Crime(s)	SM Platform(s)	Location	Primary Source
1	2013	Murder	Badoo	London, England	NY Post
2	2014	Rape	Tinder	Baton Rouge, LA	The Advocate
3	2014	Blackmail and Libel	Tinder	Houston, TX	NY Post
4	2014	Rape	Tinder	Dublin, Ireland	Irish Times
5	2014	Stalking, Attempted Kidnapping	Twitter	Bristol, England	Mirror
6	2014	Gang Rape	Tinder	Sydney, Australia	The Sydney Morning Herald
7	2014	Rape and Stalking	Tinder	Gainesville, FL	The Gainesville Sun
8	2014	Assault, Burglary	Tinder	Townsville, Australia	Townsville Bulletin
9	2015	Rape	Tinder	Denver, CO	Fox 31 (Denver)
10	2015	Sexual Assault	Tinder	Denver, CO	CBS Denver (CBS4)
11	2015	Theft	Tinder	Denver, CO	Fox31 Denver
12	2015	Rape	Facebook	Australia	PerthNow
13	2015	Armed Robbery	Facebook	Allentown, PA	Lehigh Valley Live
14	2015	Robbery	Tinder	Morisset, Australia	Daily Mail
15	2015	Stalking, Harassment	Tinder	Horry County, SC	WMBF News
16	2015	Burglary	Instagram	Orange County, CA	The Washington Times

Event	Year*	Crime(s)	SM Platform(s)	Location	Primary Source
17	2015	Armed Robbery	Tinder	Fresno, CA	ABC 30 Action News
18	2015	Rape	Tinder	Wellington, New Zealand	Stuff
19	2015	Human Trafficking	Instagram	Toronto, Canada	Global News
20	2015	Armed Robbery	Instagram	Philadelphia, PA	CNBC / Philadelphia Daily News
21	2015	Serial Murders	Grindr & Others	London, England	Birmingham Mail
22	2016	Armed Robbery	Meetme, Tinder	Vancouver, WA	KATU 2 (Portland)
23	2016	Armed Robbery, Aggravated Assault	Facebook	Columbus, GA	Columbus Ledger-Enquirer
24	2016	Kidnapping, Assault	Tinder	University of Kansas	USA Today
25	2016	Armed Robbery	Tinder, Craigslist	Boulder, CO	Fox 31 (Denver)
26	2016	Sexual Assault	Tinder	Seattle, WA	Seattle PI
27	2016	Armed Robbery, Assault	Facebook	Lauderdale, MN	Pioneer Press (St. Paul, MN)
28	2016	Stalking, Harassment	Unknown	UK	The Sun
29	2016	Rape/Sexual Assault	Tinder	Denver, CO	CBS Denver (CBS4)
30	2016	Burglary	Facebook	Austin, TX	KXAN (Austin)
31	2016	Rape, Sexual Assault, Human Trafficking	Facebook	Coventry, England	Daily Mail
32	2016	Stalking, Harrassment	Facebook	Lancaster, PA	PennLive

Event	Year*	Crime(s)	SM Platform(s)	Location	Primary Source
33	2016	Murder, Robbery	Plenty of Fish	Auburndale, FL	WTSP-TV (Tampa) / USA Today
34	2016	Rape	Tinder	Chester, England	Warrington Guardian
35	2016	Armed Robbery	Instagram, Snapchat	Paris, France	Irish Examiner
36	2016	Rape	Tinder	Pleasant Grove, UT	Herald Extra
37	2016	Unlawful Restraint, Aggravated Battery	Tinder	River Forest, IL	Chicago Tribune
38	2016	Cyberstalking	Instagram, Twitter	Doylestown, PA	NBC Philadelphia
39	2016	Burglary, Grand Larceny	Tinder	South Nyack, NY	CBS New York
40	2016	Aggravated Robbery, Sexual Assault	Tinder	Bolingbrook, IL	The Herald-News
41	2016	Murder	Tinder	Colorado Springs, CO	The Daily Dot
42	2016	Rape	Tinder	New Orleans, LA	The Advocate
43	2016	Armed Robbery, Shooting	Facebook	Peoria, IL	Peoria Journal Star
44	2016	Rape of a Minor	Tinder	London, England	London Evening Standard
45	2016	Armed Robbery, Sexual Assault	Tinder	Sandy Springs, GA	Atlanta Journal-Constitution
46	2016	Murder	Tinder	Mexico City, Mexico	SFGate
47	2016	Rape	Tinder, WhatsApp	Newcastle, England	Telegraph
48	2016	Rape of a Minor	Facebook	Callaway County, MO	ABC 17 News

Event	Year*	Crime(s)	SM Platform(s)	Location	Primary Source
49	2016	Armed Robbery	Tinder	Louisville, KY	LEX-18
50	2016	Armed Robbery	Facebook	Wilmington, MA	Wilmington Patch
51	2016	Armed Robbery	Tinder	Boulder, CO	Denver 7 News
52	2016	Rape	Tinder	Brisbane, Australia	The Courier-Mail
53	2016	Robbery, Aggravated Battery	Facebook	Chicago, IL	Chicago Tribune
54	2016	Rape	Tinder	Kowloon, Hong Kong	EJ Insight
55	2016	Assault, Auto Theft	Instagram	Los Angeles, CA	KTLA-5
56	2017	Murder	Facebook	Nairobi, Kenya	Nairobi News
57	2017	Armed Robbery	Facebook	Milwaukee, WI	Fox 6 (Milwaukee)
58	2017	Robbery	Facebook	Tulsa, OK	KFOR-TV (Oklahoma City)
59	2017	Armed Robbery	Plenty of Fish, Tinder	Omaha, NE	The Daily Nonpareil (Council Bluffs, IA)
60	2017	Rape	Tinder	Huntingburg, IN	Chattanooga Times Free Press
61	2017	Burglary	Instagram	Brentwood, CA	Us Weekly
62	2017	Gang Rape	Facebook	Kisumu. Kenya	The Standard
63	2017	Armed Robbery	Facebook	Grand Rapids, MI	WZZM 13 (Grand Rapids, MI)
64	2017	Human Trafficking	Instagram	Vacaville, CA	East Bay Times

Event	Year*	Crime(s)	SM Platform(s)	Location	Primary Source
65	2017	Armed Robbery	Facebook	Hammond, IN	The Times of Northwest Indiana
66	2017	Rape, Blackmail	Facebook	Virtual - UK, US, Australia	Th Guardian
67	2017	Burglary	Instagram	Surrey, England	Daily Mail
68	2017	Rape	Tinder	Tampa, FL	WFLA News Channel 8 (Tampa, FL)
69	2017	Murder, Robbery	Unknown	Houston, TX	New York Daily News
70	2017	Armed Robbery	Meetme	Auburndale, FL	WFTS -ABC Action News (Tampa, FL)
71	2017	Rape	Tinder	St. George, UT	The Spectrum
72	2017	Rape	Facebook	Port Elizabeth, South Africa	The Citizen
73	2017	Rape and Extortion	Facebook	Caloocan City, Philippines	GMA Network
74	2017	Armed Robbery	Facebook	Grand Rapids, MI	MLive
75	2017	Criminal Confinement, Theft	Facebook	Indiana	Atlanta Journal-Constitution
76	2017	Armed Robbery	Facebook	Brunswick, GA	The Brunswick News
77	2017	Armed Robbery	Tinder	Gothenburg, Sweden	The Local
78	2017	Burglary	Instagram	Los Angeles, CA	News.Com.Au
79	2017	Cyberstalking and Harassment	Unknown	Staten Island, NY	NY Daily News
80	2017	Armed Robbery	Facebook	Anntioch, TN	WKRN

Event	Year*	Crime(s)	SM Platform(s)	Location	Primary Source
81	2017	Rape	Instagram, Snapchat	Germantown, MD	The Washington Post
82	2017	Armed Robbery	Facebook	Tucson, AZ	KVOA News-4 Tucson
83	2017	Gang Rape, Child Pornography	Facebook	Mongmong, Guam	Pacific News Center
84	2017	Armed Robbery	Tinder, MeetMe	Morristown, TN	WVLT Local 8 (Knoxville)
85	2017	Armed Robbery	Facebook	New York, NY	Fox News
86	2017	Robbery	Tinder	Springfield, OR	Seatle Times
87	2017	Child Sex Trafficking	Facebook	Phoenix, AZ	The Republic
88	2017	Armed Robbery	Unknown	Whitewater, WI	Daily Union
89	2017	Rape	Tinder	Palmerston North, New Zealand	Stuff
90	2017	Armed Robbery	Beetalk	Sandakan, Malaysia	New Straits Times
91	2017	Theft	Tinder	Phoenix, AZ	ABC 15
92	2017	Theft	Tinder	Leonia, NJ	ABC 6 WPVI-TV (Philadelphia)
93	2017	Armed Robbery, Assault	Unknown	Sacramento, CA	Fox 40
94	2017	Rape	Tinder	South Hadley, MA	Mass Live
95	2017	Cyberstalking	Facebook	Cumbernauld, Scotland	Elite Daily
96	2017	Armed Robbery, Carjacking, Shooting	MeetMe	Daytona Beach, FL	The Grio

Event	Year*	Crime(s)	SM Platform(s)	Location	Primary Source
97	2017	Rape of a Minor	Tinder	Johnson City, TN	WJHL News Channel 11
98	2017	Robbery	Tinder	Breckenridge, CO	Summit Daily
99	2017	Armed Robbery	SnapChat	Coral Springs, FL	Sun Sentinel
100	2017	Assault, Robbery	Tinder	Amherst, OH	Morning Journal
101	2017	Robbery	Tinder	Sydney, Australia	ABC News (Australian Broadcasting Corporation)
102	2017	Rape, Assault, Imprisonment	Tinder	Melbourne, Australia	Daily Mail
103	2017	Abduction, Grand Larceny	Facebook	Caroline County, VA	WRIC-8 ABC News
104	2017	Armed Robbery	Tinder	Longview, TX	Longview News-Journal
105	2017	Human Trafficking, Sodomy	Facebook	Cullman County, AL	WHNT-19 News
106	2017	Stabbing, Attempted Carjakcing	Tinder	Melbourne, Australia	Stuff (Check source)
107	Unknown	Cyberstalking	Facebook	Stoke Gifford, England	BristolPost
108	Unknown	Burglary	Facebook	Unknown	Sileo
109	Unknown	Murder, Stalking	Tinder	Brisbane, Australia	Daily Mail
110	Unknown	Cyberstalking	Instagram	Unknown	Teen Vogue
111	Unknown	False Imprisonment	SeekingArrangement	Sandy Springs, GA	11 Alive (Atlanta)

**Most recent year listed for crimes spanning multiple years*

References

2 men in Vancouver set up dates online, get robbed by armed masked men. (n.d.). Retrieved September 30, 2017, from http://komonews.com/news/local/2-men-in-vancouver-set-up-dates-online-get-robbed-by-armed-masked-men

Alarm in Kisumu as women fall victims to Facebook criminals. (2017, September 06). Retrieved September 17, 2017, from https://www.standardmedia.co.ke/business/article/2001253708/facebook-date-rape-hits-rocky-village-hill

Alba, A. (2017, May 23). New 'Gatsby' Dating App Blocks Criminals And Sex Offenders. Retrieved September 30, 2017, from http://www.vocativ.com/432322/gatsby-dating-app-blocks-criminals/index.html

Alexander, S. (2016, November 03). Dating apps in record number of offences this year. Retrieved September 30, 2017, from https://www.thesun.co.uk/news/2106434/fifty-sex-crimes-involving-dating-apps-tinder-and-grindr-reported-to-the-met-police-in-london-in-record-year-for-offences/

Awford, J. (2017, February 16). Tinder stalker stabbed date 11 times, then doused her in gasoline. Retrieved September 29, 2017, from http://nypost.com/2017/02/16/tinder-stalker-stabbed-date-11-times-then-doused-her-in-gasoline/

Baynes, C. (2016, November 14). Obsessed stalker jailed for plot to kidnap woman he met online and keep her as ‘sex slave.’ Retrieved September 29, 2017, from http://www.mirror.co.uk/news/uk-news/obsessed-stalker-jailed-plot-kidnap-9258168

Becker, T. (2016, November 23). Tinder date turns to carjacking in Vancouver. Retrieved September 30, 2017, from http://koin.com/2016/11/22/tinder-date-turns-to-carjacking-in-vancouver/

Bestselling psychological thriller author. (n.d.). Retrieved November 11, 2017, from https://claremackintosh.com/clare-mackintosh-about/

Blake, A. (2016, February 25). Burglar used Facebook, Instagram posts to find victims: Prosecutors. Retrieved October 21, 2017, from http://www.washingtontimes.com/news/2016/feb/25/burglar-used-facebook-and-instagram-posts-find-vic/

Bolerjack, D. (n.d.). Tinder date leads to alleged rape of Dixie State University student. Retrieved September 30, 2017, from http://kutv.com/news/local/tinder-date-leads-to-alleged-rape-of-dixie-state-university-student

Briscoe, T. (2017, January 23). Violent robbery started as scam drug buy on Facebook, prosecutors say. Retrieved September 09, 2017, from http://www.chicagotribune.com/news/local/breaking/ct-violent-cragin-facebook-robbery-20170122-story.html

Brown, J. (2017, August 06). Houston Man Says 'Nightmare' Tinder Date Accused Him Of Rape, Blackmailed Him For $10,000. Retrieved September 30, 2017, from https://www.inquisitr.com/4412563/houston-tinder-date-from-hell-blackmail/

Bult, L. (2016, May 12). Kansas sorority girl kidnapped and beaten by Tinder date. Retrieved September 30, 2017, from http://www.nydailynews.com/news/national/kansas-sorority-girl-kidnapped-beaten-tinder-date-article-1.2634879

Burbrink, J. (2017, February 16). Police warn about burglaries during funeral services. Retrieved October 22, 2017, from http://www.wpta21.com/story/34525576/police-warn-about-burglaries-during-funeral-services

Burns, J. (2017, June 23). Finally, the perfect app for superfans, stalkers, and serial killers. Retrieved September 29, 2017, from https://www.forbes.com/sites/janetwburns/2017/06/23/finally-the-perfect-dating-app-for-superfans-stalkers-and-serial-killers/#2575d13ef166

Carlson, A. (2017, March 11). Suspected Human Trafficker Allegedly Held 6 Women in $1M Atlanta Mansion and Made Them Work at Strip Clubs. Retrieved October 21, 2017, from http://people.com/crime/atlanta-mansion-human-trafficking-women-dance-strip-clubs/

Cerullo, M. (2017, August 08). Cousins linked to murders of two Houston-area men. Retrieved September 30, 2017, from http://www.nydailynews.com/news/crime/cousins-linked-murders-houston-area-men-article-1.3394080

Christie, S. (2017, July 28). How 'Insta-bragging' could soon invalidate your insurance. Retrieved September 17, 2017, from http://www.telegraph.co.uk/money/consumer-affairs/insta-bragging-could-soon-invalidate-insurance/

Clarke-Billings, L. (2016, November 18). What do Tinder's new gender identity options mean? Retrieved October 22, 2017, from http://www.newsweek.com/what-do-tinders-37-new-gender-identity-options-mean-522679

Culley, J. (2017, July 27). Facebook holidays burglary shock: Travel Brits boasting from airports face home raids. Retrieved September 09, 2017, from https://www.dailystar.co.uk/travel/travel-news/633023/summer-holiday-2017-airport-uk-social-media-burglary

Damiani, M. L. (2014). Location privacy models in mobile applications: conceptual view and research directions. *GeoInformatica, 18*(4), 819-842. doi:10.1007/s10707-014-0205-7

Dating safely. (n.d.). Retrieved October 22, 2017, from https://www.gotinder.com/safety?locale=en

Donald, K. (2017, September 04). British paedophile Paul Leighton jailed for 16 years for rape. Retrieved September 17, 2017, from https://www.theguardian.com/uk-news/2017/sep/04/british-paedophile-paul-leighton-jailed-for-16-years-for-rape

Eustachewich, L. (2017, August 10). Former male escort convicted in dating app murder. Retrieved September 30, 2017, from http://nypost.com/2017/08/10/former-male-escort-convicted-in-dating-app-murder/

Evans, M. (2016, August 09). Rugby star accused of raping girl he met on Tinder cleared of all charges. Retrieved September 12, 2017, from http://www.telegraph.co.uk/news/2016/08/09/rugby-star-accused-of-raping-girl-he-met-on-tinder-cleared-of-al/

'Facebook killer' arraigned in court for murder charge. (2017, September 01). Retrieved September 29, 2017, from http://nairobinews.nation.co.ke/news/facebook-killer-murder-charge/

French, M. (2017, October 15). Alanis Morissette Robbed of $2 Million Worth of Jewelry: Report. Retrieved September 09, 2017, from http://www.usmagazine.com/celebrity-news/news/alanis-morissette-robbed-of-2-million-worth-of-jewelry-report-w467042

Gander, K. (2016, February 22). The 12 worst Tinder horror stories. Retrieved September 29, 2017, from http://www.independent.co.uk/life-style/love-sex/tinder-a6784271.html

Greenwood, S., Perrin, A., & Duggan, M. (2016, November 11). Social Media Update 2016. Retrieved July 23, 2017, from http://www.pewinternet.org/2016/11/11/social-media-update-2016/

Gundran, R. (2017, September 26). Mesa police arrest 2 men in child sex trafficking investigation. Retrieved September 29, 2017, from http://azc.cc/2yqI9YD

Halsne, C., & Koeberl, C. (2016, November 03). Blinders on: Denver DA refused 7 of 10 felony rape cases. Retrieved September 30, 2017, from http://kdvr.com/2016/11/03/blinders-on-denver-da-refused-7-of-10-felony-rape-cases/

Hardy, R. (2017, October 20). Why were false rape claims allowed to ruin the life of a hero PC? Officer describes ‘sheer hell’ after being wrongly accused of attack by woman he met on Plenty of Fish dating site. Retrieved October 22, 2017, from http://www.dailymail.co.uk/news/article-5002324/Why-false-rape-claims-allowed-ruin-hero-PC-s-life.html

Havens, E. (2017, August 21). DSU student testifies against alleged rapist with a history in Utah. Retrieved September 30, 2017, from http://www.thespectrum.com/story/news/local/2017/08/21/dsu-student-testifies-against-alleged-rapist-history-utah/587090001/

Hensley, N., Keshner, A., & Annese, J. (2017, April 10). Internet 'Satan' busted on S.I. after decades of harassment. Retrieved September 8, 2017, from http://www.nydailynews.com/new-york/internet-satan-busted-s-decades-harassment-article-1.3041247

Here's why celebrities should be careful sharing their holiday photos. (2017, July 24). Retrieved September 09, 2017, from http://www.news.com.au/entertainment/celebrity-life/celebrity-selfies/hilary-duff-robbed-after-instagram-holiday-post/news-story/5cdc651d441b6f483e1cf50f2c4147ca

Hoggard, C. (2015, December 01). Tinder bait & switch leads to Fresno armed robbery & auto theft. Retrieved October 09, 2017, from http://abc30.com/news/tinder-bait-and%20switch-leads-to-fresno-armed-robbery-and%20auto-theft/1104629/

Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study. (2017, February 01). Retrieved July 23, 2017, from https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new

Identity Theft Assessment and Prediction Report 2017 (Rep. No. 1706). (2017). Austin, TX: The University of Texas at Austin Center for Identity.

Introducing more genders on Tinder. (2016, November 15). Retrieved October 22, 2017, from blog.gotinder.com/genders/

Jain, A. K., & Shanbhag, D. (2012). Addressing Security and Privacy Risks in Mobile Applications. *IT Professional, 14*(5), 28-33. doi:10.1109/mitp.2012.72

Jechow, A., & Rangel, L. (2017, January 12). Facebook comment leads to burglary, teen's assault. Retrieved September 09, 2017, from http://kxan.com/2017/01/11/burglary-assault-started-with-facebook-live-comment-police-say/

Johnson, A. (2015, February 09). Instagram posts lead to robbery. Retrieved September 09, 2017, from https://www.cnbc.com/2015/02/09/valuables-posted-on-instagram-lead-to-robbery.html

Jones, R. (2017, April 28). Teenager Faces Charges After Setting Up Sneaker Robbery on Facebook. Retrieved September 09, 2017, from http://footwearnews.com/2017/focus/athletic-outdoor/teenager-faces-charges-facebook-sneaker-robbery-air-jordan-11-space-jam-344437/

Jurgens, D., Finnethy, T., McCorriston, J., Xu, Y. T., & Ruths, D. (2015). Geolocation prediction in Twitter using social networks: a critical analysis and review of current practice. In *Proceedings of the ninth international conference on web and social media* (pp. 188-197). Palo Alto, CA: AAAI Press. Retrieved July 26, 2017, from http://www.derekruths.com/static/publication_files/JurgensEtAl_ICWSM2015.pdf

Kemp, S. (2017, January 24). Digital in 2017: Global Overview. Retrieved July 23, 2017, from https://wearesocial.com/special-reports/digital-in-2017-global-overview

Khan, S. (2016, February 7). Rapes linked to online dating up by more than 450% in five years. Retrieved September 30, 2017, from http://www.independent.co.uk/news/uk/home-news/rapes-linked-to-online-dating-up-by-more-than-450-in-five-years-a6858826.html

Khloe Kardashian: Kim's robbery was God's way of teaching us about security. (2017, August 13). Retrieved September 09, 2017, from http://www.irishexaminer.com/breakingnews/entertainment/khloe-kardashian-kims-robbery-was-gods-way-of-teaching-us-about-security-801845.html

Klecker, M. (2017, September 28). After spate of robberies, police warn users of dating apps: Be cautious when arranging meetups. Retrieved September 30, 2017, from http://www.nonpareilonline.com/news/crime/after-spate-of-robberies-police-warn-users-of-dating-apps/article_7d6fab6e-a466-11e7-8cd4-dbf0211f611d.html

Lally, C. (2016, October 26). Burglars trawl Facebook, Twitter for targets, gardaí say. Retrieved September 09, 2017, from https://www.irishtimes.com/news/crime-and-law/burglars-trawl-facebook-twitter-for-targets-garda%C3%AD-say-1.2843286

Lang, N. (2016, November 17). The danger of Tinder's LGBT-friendly upgrade: How the dating app could be used to target trans users. Retrieved September 30, 2017, from https://www.salon.com/2016/11/17/the-danger-of-tinders-lgbt-friendly-upgrade-how-the-dating-app-could-be-used-to-target-trans-users/

Legaspi, A. (2017, July 28). Facebook friend nabbed for extortion, rape of 17-year-old. Retrieved September 17, 2017, from http://www.gmanetwork.com/news/news/metro/619873/facebook-friend-nabbed-for-extortion-rape-of-17-year-old/story/

Leighton, H. (2016, December 27). Reports: Man allegedly kills Tinder date then dissolves her body in acid. Retrieved September 30, 2017, from http://www.sfgate.com/crime/article/Reports-Man-arrested-after-allegedly-murdering-10820356.php

Ludwig, A. (2016, September 20). Panty Raid Foiled: Instagram Burglar Gets Prison for Stalking OC Coeds. Retrieved September 17, 2017, from https://patch.com/california/fountainvalley/panty-raid-foiled-instagram-burglar-gets-prison-stalking-oc-co-eds

Mackintosh, C. (2016). *I see you*. Rearsby, Leicester: WF Howes Ltd.

Martin, K., & Shilton, K. (2016). Putting mobile application privacy in context: An empirical study of user privacy expectations for mobile devices. *The Information Society, 32*(3), 200-216. doi:10.1080/01972243.2016.1153012

Martinez, J. (2017, January 29). Mastermind Behind Kim Kardashian's Paris Robbery Reveals How Jewelry Was Sold. Retrieved September 09, 2017, from http://www.complex.com/pop-culture/2017/01/mastermind-behind-kim-kardashian-paris-robbery-reveals-how-jewelry-was-sold

Mcallister, T. (2017, July 25). Sad Hilary Duff Instagram burglary victim: Why'd I post those vacation photos? Retrieved September 17, 2017, from https://mynewsla.com/crime/2017/07/24/hilary-duff-posts-instagram-vacation-pics-burglars-tipped-off-empty-north-hollywood-hills-home-targeted/

Mcdade, M., & Kurzweil, A. (2017, May 9). Woman shares details of L.A. assault during date with man she met on Instagram. Retrieved September 17, 2017 from http://ktla.com/2017/05/08/woman-shares-details-of-assault-during-date-with-man-she-met-on-instagram/

Miller, M. (2017, January 04). Facebook stalker pleads guilty in bizarre case that left victim besieged by prostitutes. Retrieved September 8, 2017, from http://www.pennlive.com/news/2017/01/facebook_stalker_pleads_guilty.html

Molinari, S. (2017, May 23). Technology's role in human trafficking cannot be ignored. Retrieved September 29, 2017, from http://thehill.com/blogs/pundits-blog/lawmaker-news/334732-technologys-role-in-human-trafficking-cannot-be-ignored

Moore, C. (2017, March 06). Burglars ransack 'shaken' footballer John Terry's £5m mansion after he posts pictures of his family skiing holiday on Instagram. Retrieved September 17, 2017, from http://www.dailymail.co.uk/news/article-4280436/Burglars-ransack-John-Terry-s-mansion.html

Morgan, R., & White, N. (2016, November 12). 'I was very creeped out': Blogger who travels the world posting breathtaking photos on Instagram discovers that a woman is following her and taking the exact SAME images. Retrieved September 08, 2017, from http://www.dailymail.co.uk/femail/article-3927672/I-creeped-Blogger-travels-world-posting-breathtaking-photos-Instagram-discovers-woman-following-taking-exact-images.html

Ng, K. (2016, January 11). Tinder and Grindr: Warning over dating app risks as crimes like 'sextortion' and rape increases. Retrieved September 30, 2017, from http://www.independent.co.uk/news/uk/crime/warning-over-dating-app-dangers-as-crimes-like-sextortion-and-rape-increases-mentions-of-tinder-and-a6805601.html

Noll, J. (2017, March 13). Sisters of Struggle: Being a 'Diamond Kitty'. Retrieved September 29, 2017, from http://www.11alive.com/article/news/crime/sisters-of-struggle-being-a-diamond-kitty/85-421494186

Norris, P. (2017, August 03). Dating app warning after woman drugged and sexually assaulted after going to meet man who'd offered to cook for her. Retrieved September 30, 2017, from http://www.gloucestershirelive.co.uk/news/gloucester-news/woman-drugged-sexually-assaulted-after-274451

Norway sees more rapes tied to Tinder use. (2016, February 19). Retrieved September 30, 2017, from https://www.thelocal.no/20160219/norway-seeing-more-rapes-in-connection-with-tinder

Omaha police: string of armed robberies linked to dating apps. (2017, September 28). Retrieved September 30, 2017, from http://www.waow.com/story/36479711/omaha-police-string-of-armed-robberies-linked-to-dating-apps

Partridge, E. (2014, October 08). Police warning after Tinder date ends in gang rape in Sydney. Retrieved September 30, 2017, from http://www.smh.com.au/nsw/police-warning-after-tinder-date-ends-in-gang-rape-in-sydney-20141008-1138ef.html

Pending rape case of 'Facebook killer' unearthed. (2017, September 14). Retrieved September 17, 2017, from http://nairobinews.nation.co.ke/news/rape-case-facebook-killer-unearthed/

Pratt, J. H., & Conger, S. (2009). Without Permission: Privacy on the Line. *International Journal of Information Security and Privacy, 3*(1), 30-44. doi:10.4018/jisp.2009010103

Raising awareness about over-sharing. (n.d.). Retrieved July 26, 2017, from pleaserobme.com

Ramseth, L. (2017, May 1). St. George man charged with rape; Dixie State police chief sees a pattern. *The Salt Lake Tribune*. Retrieved September 30, 2017 from archive.sltrib.com/article.php/id=5230870&itype=CMSID

Rieck, D., & Landis, K. (2017, May 24). Burglars hit homes as families grieve at funeral services. Retrieved October 22, 2017, from http://www.bnd.com/news/local/article152344332.html

Roose, K. (2017, September 21). Facebook's Frankenstein Moment. Retrieved September 29, 2017, from https://www.nytimes.com/2017/09/21/technology/facebook-frankenstein-sandberg-ads.html

Rossen, J., & Davis, J. (2013, June 13). Thieves ransack homes of families attending funerals. Retrieved September 9, 2017, from https://www.today.com/news/thieves-ransack-homes-families-attending-funerals-6C10280103

Seals, G. (2016, November 15). This Mystery Girl Followed a Travel Blogger Across the Globe and Recreated Her Instagrams in Creepy Detail. Retrieved September 08, 2017, from http://www.teenvogue.com/story/instagram-blogger-copy-cat

Sears, A. (2017, June 30). "Don't let your guard down:" Man robbed at gunpoint during Facebook Marketplace purchase. Retrieved September 09, 2017, from http://fox6now.com/2017/06/30/dont-let-your-guard-down-man-robbed-at-gunpoint-while-buying-moped-through-facebook-marketplace/

Shapiro, E. (n.d.). String of armed robberies linked to dating apps, Omaha police say. Retrieved September 30, 2017, from http://abcnews.go.com/US/string-armed-robberies-linked-dating-apps-omaha-police/story?id=50152572

Siegler, M. G. (2010, February 17). Please Rob Me makes Foursquare super useful for burglars. Retrieved July 3, 2017, from https://techcrunch.com/2010/02/17/please-rob-me-makes-foursquare-super-useful-for-burglars/

Silver, C. (2016, June 28). How Facebook's 'People You May Know' Section Just Got Creepier. Retrieved September 08, 2017, from https://www.forbes.com/sites/curtissilver/2016/06/28/how-facebooks-people-you-may-know-section-just-got-creepier/

Smithers, R. (2017, August 18). Former burglars say barking dogs and CCTV are best deterrent. Retrieved September 17, 2017, from https://www.theguardian.com/business/2017/aug/18/former-burglars-barking-dogs-cctv-best-deterrent

Spicer, M. (Director). (2017). *Ingrid Goes West* [Motion picture on Streaming Video (Amazon)]. US: Neon.

Spotlight changes the way law enforcement investigates sex trafficking. (n.d.). Retrieved November 03, 2017, from https://www.htspotlight.com/apps/

Tindstagramming is the creepy new way to stalk someone on social media. (2017, September 27). Retrieved September 29, 2017, from http://www.news.com.au/technology/online/social/tindstagramming-is-the-creepy-new-way-to-stalk-someone-on-social-media/news-story/77f3a242d30f

Traffickers use social media to target victims. (2017, February 19). Retrieved September 29, 2017 from http://wspa.com/2017/02/19/traffickers-use-social-media-to-target-victims/

Tulp, S. (2016, July 25). A University of Kansas student has terrifying Tinder encounter. Retrieved September 30, 2017, from http://college.usatoday.com/2016/05/18/tinder-date-university-kansas/

Vanden Heuvel, A., & Norsworthy, C. (2016, March 06). Safety issues arise with social meet-up apps. Retrieved September 30, 2017, from http://www.redandblack.com/athensnews/safety-issues-arise-with-social-meet-up-apps/article_081b2b18-e35b-11e5-86a7-9b31afac0a28.html

Vezner, T. (2017, April 7). Charges: First a date on social media, then armed robbery. Retrieved September 9, 2017 from http://www.twincities.com/2017/04/07/charges-first-a-date-on-social-media-then-armed-robbery/

Want to find someone? Do a confidential people search to find their contact info! (n.d.). Retrieved November 04, 2017, from http://www.intelius.com/

Wassef, M. (2017, June 06). Feds offer plea deal to New Brighton man accused of sending disturbing threats to 2 women. Retrieved October 22, 2017, from http://www.silive.com/news/2017/06/feds_offer_plea_deal_to_new_br.html

Webcam Child Sex Tourism (Rep.). (2013, April 11). Retrieved September 30, 2017, from Terre des Hommes website: https://www.terredeshommes.nl/en/publications/webcam-child-sex-tourism

Werber, C. (2017, March 30). Nobody knows how dangerous online dating really is-and dating sites won't talk about it. Retrieved September 30, 2017, from https://qz.com/890320/nobody-know-how-dangerous-online-dating-really-is-and-dating-sites-wont-talk-about-it/

White, N., & Cleary, B. (2016, November 10). EXCLUSIVE: 'That could have been me': Fourth woman reveals her horror after realising the man who stalked her on Tinder and invited her to his 'hot tub' stabbed his ex-girlfriend 11 times. Retrieved September 29, 2017, from http://www.dailymail.co.uk/news/article-3922100/Fourth-woman-says-Paul-Lambert-stalked-Brisbane-met-Tinder-months-stabbed-Angela-Jay-11-times.html

Williams, C., & Chi, H. (2015). An investigation of privacy protocols in location-based service. *Proceedings of the 2015 Information Security Curriculum Development Conference on - InfoSec 15*. doi:10.1145/2885990.2886005